AUTOMATION ANYWHERE

로봇 프로세스 자동화를 위한 엔터프라이즈급 보안

소개

비즈니스 프로세스 자동화 기술에 투자한 지 20년 이상이 지났는데 자동화된 작업이 20% 미만에 불과한 이유는 무엇입니까? 가장 큰 이유는 엔터프라이즈 시스템의 85%에서 제대로 정의된 API가 부족하기 때문입니다. 그 결과, 비즈니스 라인의 통합 요청에 대한 IT 백로그가 점차 증가하고 있습니다.

로봇 프로세스 자동화는 비즈니스 사용자가 인간과 마찬가지로 엔터프라이즈 시스템과 상호 작용할 수 있는 소프트웨어 봇을 생성할 수 있다는 비전을 바탕으로 탄생했습니다. RPA 봇은 인간과 마찬가지로 자격 증명을 사용하여 엔터프라이즈 애플리케이션에 로그인하고 API가 없는 레거시 애플리케이션을 비롯하여 모든 엔터프라이즈 애플리케이션과 관련된 작업을 자동화할 수 있습니다. 청구 처리, 대출 처리, 계정 조정, 송장 생성/제출 및 보고서 생성은 다양한 비즈니스 분야에 걸쳐있는 잠재적인 자동화의 몇 가지 예시일 뿐입니다.

상당한 시간 및 비용 절감, 고객 만족도 향상, 직원 사기 향상, RPA를 사용하여 경쟁업체보다 압도적인 경쟁 우위를 구축할 수 있는 능력에 대한 가능성을 확인하는 것은 어렵지 않습니다. 그러나 이러한 이점의 완전한 실현은 엔터프라이즈급 솔루션의 사용 여부에 달려 있습니다.

견고한 안정성, 확장성 및 적용 가능성과 유용성을 극대화하기 위한 광범위한 기능 세트의 제공은 자동화의 필수 조건 중 일부입니다. 그러나 이러한 요소는 비즈니스의 가장 중요한 요구 사항인 end-to-end 보안을 다루지 않습니다. 중요한 앱과 민감한 관련 데이터에 대한 end-to-end 보호 기능을 제공하면서 최소 권한 및 업무 분리 등의 핵심 원칙을 완벽하게 지원할 수 있는 기능을 갖춘 강력한 보안 아키텍처는 업무에 중요합니다.

이 문서에서는 시장을 선도하는 디지털 인력 플랫폼인 Automation Anywhere Enterprise에서 설명한 대로 엔터프라이즈급 보안을 위한 업계 최고 표준의 개요를 제공합니다.

“상당한 시간 및 비용 절감, 고객 만족도 향상, 직원 사기 향상, RPA를 사용하여 경쟁업체보다 압도적인 경쟁 우위를 구축할 수 있는 능력에 대한 가능성을 확인하는 것은 어렵지 않습니다. 그러나 이러한 이점의 완전한 실현은 엔터프라이즈급 솔루션의 사용 여부에 달려 있습니다.

아키텍처 및 운영

엔터프라이즈급 RPA 구현에 필요한 보안 제어를 이해하는 것은 솔루션과 해당 작업을 구성하는 구성요소에 대한 이해 여부에 달려 있습니다.

주요 구성 요소

그림 1과 같이 Automation Anywhere Enterprise의 주요 구성 요소는 Control Room, Bot Creator, 봇 실행자입니다.

Control Room

Control Room은 자동화 환경의 두뇌 역할을 합니다. Control Room은 Windows 서버 기반의 관리 시스템으로, 통합 데이터베이스가 있어 전반적인 시스템 관리를 총체적으로 확인할 수 있습니다. 또한 Control Room은 RPA 운영자가 디지털 인력을 오케스트레이션, 즉 조직의 봇 운영을 예약, 배포, 실행, 모니터링, 관리하기 위한 곳이기도 합니다. 게다가 버전 제어 기능(Apache Subversion Server)이 내장되어 있어 변경 관리 모범 사례를 적용하고 프로덕션 준비 봇의 중앙 집중식 저장소를 구축하는 동시에 다중 사용자 협업을 용이하게 합니다.

Bot Creator

Bot Creator는 봇을 구축하는 데 사용됩니다. 워크스테이션 클래스 또는 가상 머신에서 실행되는 Windows 데스크톱 앱인 Bot Creator는 비즈니스 프로세스 전문가가 자동화를 생성하고 테스트하는 데 사용됩니다. 봇은 봇 편집자를 사용하여 생성되며 로컬, 비프로덕션 테스트 데이터 및 앱 인스턴스를 사용하는 봇 테스트는 Bot Runner에 의해 구현됩니다. 성능, 데이터 무결성, 보안 등에 대한 성공적인 테스트를 마치면 봇은 Control Room 저장소에 체크인되어 프로덕션 배포에 사용할 수 있게 됩니다.

Bot Runner

Bot Runner는 봇을 작동시킵니다. Bot Creator와 동일한 애플리케이션 코드를 사용하지만 다른 라이선스 키를 사용하는 Bot Runner는 프로덕션 환경에서 대상 애플리케이션 및 프로덕션 데이터 저장소의 프로덕션 인스턴스를 사용하여 봇을 실행합니다. 실제로 봇 실행자는 생성 및 편집 기능을 사용할 수 없으므로 봇 실행만이 수행할 수 있는 유일한 작업입니다. 신뢰성이 뛰어난 대규모 작업의 경우 봇 실행자의 풀링도 지원됩니다.

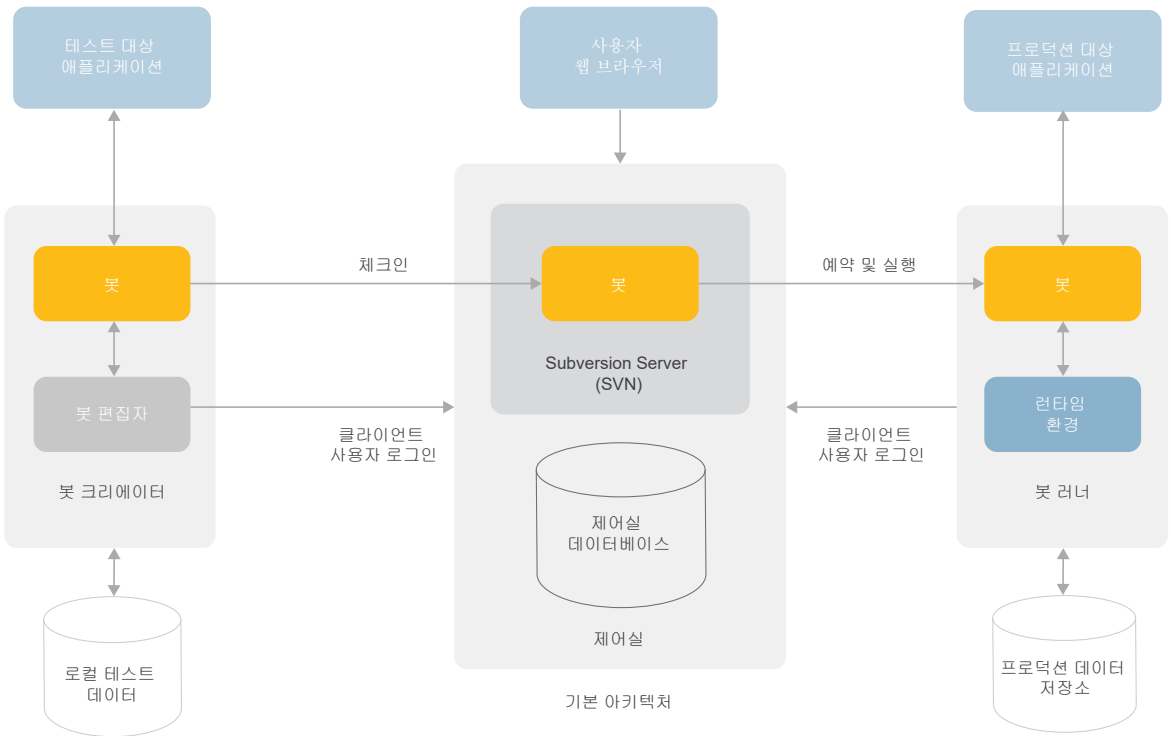

그림 1: 기본 Automation Anywhere Enterprise 아키텍처

추가 엔터프라이즈급 구성 요소

대규모 작업을 고려할 때 엔터프라이즈급 배포를 추구하는 조직과 관련된 두 가지 중요한 RPA 솔루션, 즉 온디맨드 확장 및 Bot Insight가 언급됩니다.

온디맨드 확장

Automation Anywhere Enterprise는 Amazon Web Services(AWS) 퍼블릭 클라우드를 활용하여 유연한 확대/축소, 사용량 기반 계량, 무제한 수평 확장성, Bot Runner 인프라의 지속적인 모니터링 및 감사 로깅을 비롯하여 모든 참석자 기능을 갖춘 RPA-as-a-Service를 효과적으로 제공합니다. 그 결과, 자동화 워크로드가 급격히 증가하는 경우에도 SLA 기반 성능 및 비즈니스 연속성을 지원하는 다중 노드 고가용성이 구현됩니다.

Bot Insight

Control Room 내에 완전히 통합된 서브 시스템인 Bot Insight는 봇 운영 및 비즈니스 프로세스 데이터를 거의 실시간으로 분석합니다. Bot Insight는 각 봇 고유의 고급 알고리즘을 사용하여 사용자 지정 가능한 대시보드를 자동으로 생성합니다. 세부 수준의 Bot Insight는 봇 운영에 대한 세분화된 이벤트 로그를 기반으로 제공되며 미묘한 경고, Ad-hoc 검색, 대화형 드릴다운, 시계열 분석 및 운영/비즈니스 프로세스에 대한 포괄적인 통찰력을 가능하게 합니다. 또한 추후 분석, 조사 및 보고를 위해 보안 정보 및 이벤트 관리(SIEM) 로그에 대한 모든 데이터를 내보낼 수 있습니다.

봇 실행: 두 가지 유형의 자동화

Automation Anywhere Enterprise의 고급 보안 기능을 시작하기 전에 마지막으로 명확히 해야 할 한 가지 사항은 두 가지 기본 유형의 자동화, 즉 유인 자동화와 무인 자동화입니다.

유인 자동화는 사용자가 Bot Runner 시스템에 로그인하여 봇 실행을 관찰하거나 적극적으로 지원하는 것입니다. 사용자가 필요한 이유는 봇이 작업에 도움이 되는 유틸리티 유형 기능을 제공하거나 봇이 사용자의 주기적인 입력이나 상황에 따른 지시를 요구하는 배치형 작업을 수행하기 때문일 수 있습니다. 유인 자동화는 프런트 오피스 자동화라고도 합니다.

무인 자동화는 이름에서 알 수 있듯이 비즈니스 사용자 또는 운영자 상호 작용 없이 운영됩니다. 무인 자동화는 일반적으로 봇, 자동화된 애플리케이션 또는 자동화의 목적에 대해 거의 알지 못하는 운영자에 의해 실행됩니다. 운영자는 사업부와 협력하여 봇 실행자에서 실행할 봇을 예약합니다. 실행 중에 운영자는 CPU, 메모리 및 스토리지 사용과 같은 실행 중인 봇의 운영 측면을 모니터링하여 오류나 예외 없이 실행되도록 합니다. Control Room 대시보드는 실행 중인 봇의 모든 운영 세부 사항을 표시합니다. 무인 자동화가 오류로 인해 완료되지 않으면 운영자는 자동화 문제를 해결하고 다시 시작하는 절차를 구현할 수 있습니다. 그렇지 않으면 RPA 팀 또는 사업부에 보고하여 문제를 진단하고 해결합니다.

다중 계층 엔터프라이즈 RPA 보안 다중 계층 식별 및 인증

Automation Anywhere Enterprise 보안 아키텍처의 핵심 원칙은 관련 엔터티의 사전 인증 없이 액세스 또는 작업이 허용되지 않는다는 것입니다. 이 원칙은 인간과 봇에 모두 적용됩니다. 그 결과, 유인 및 무인 자동화를 위한 다중 계층 인증 프로세스가 구현됩니다.

사용자별: 일반 엔터프라이즈 인증

자격 증명 및 페르소나는 다중 계층 방식으로 처리될 수 있습니다. 간단한 엔터프라이즈 인증 시나리오를 고려해 봅니다(**그림 2** 참조). 엔터프라이즈 사용자인 Alice는 자신의 Windows 워크스테이션을 인증합니다. 그런 다음 Alice는 원격으로 실행 중인 애플리케이션에 로그인하여 Windows 도메인 Active Directory 로그인 또는 유효한 티켓이 있는 자신의 워크스테이션을 기반으로 하는 Kerberos를 통해 인증합니다. 이 시나리오의 인증 체인에는 한 사람과 해당 자격 증명이 포함됩니다.

그림 2: 일반 엔터프라이즈 인증

이제 **그림 3**에 표시된 유인 자동화 시나리오를 고려해 봅니다. 이 경우 사용자인 Bob은 자신의 일반적인 일과의 일부로 봇을 테스트하거나 유인 자동화를 실행합니다. 1단계에서 그는 위의 Alice 시나리오와 마찬가지로 자신의 개인 자격 증명을 사용하여 Bot Runner 워크스테이션을 인증합니다. 2단계에서는 Automation Anywhere Enterprise 클라이언트를 시작하고 자신의 Control Room 사용자 ID와 암호를 입력하여 Control Room에 대한 클라이언트 소프트웨어를 인증합니다. 3단계에서는 인증을 요구하는 애플리케이션에 차례로 액세스하는 봇을 실행합니다. 이 단계에서 봇이 사용하는 자격 증명은 Enterprise 자격증명 보관에 저장되어 런타임 중에 봇에 의해 검색될 수 있으며 (동일한 도메인에 있는 Bob의 워크스테이션과 애플리케이션 서버가 제공한 여유 공간에 따라) Bob의 개인 자격 증명에 대한 패스스루가 있을 수 있습니다. 어느 쪽이든 결과적으로 총 3가지 계층의 식별 및 인증이 구현됩니다.

몇 가지 새로운 방식이 사용되었지만 **그림 4**에 표시된 무인 시나리오에 사용된 인증은 3가지 계층을 거칩니다. 이 경우 사용자인 Charles는 즉시 또는 예정된 시간에 실행할 봇을 선택할 수 있도록 Control Room을 인증하여 시작합니다.

2단계에서 봇 실행 시간이 시작되면 Control Room에서는 BotRunnerUser 자격 증명을 사용하여 Bot Runner 워크스테이션에 대한 자동 로그인을 시작합니다. 봇이 로컬 플레이어 기능으로 다운로드되고(3단계) 실행을 시작하면 BotApplicationUser 자격 증명(4단계)을 사용하여 대상 애플리케이션을 인증합니다. 유인 자동화 시나리오와 마찬가지로 BotApplicationUser 자격 증명은 자격증명 보관에서 검색되는 자격 증명이거나 BotRunnerUser 자격 증명의 패스스루일 수 있습니다.

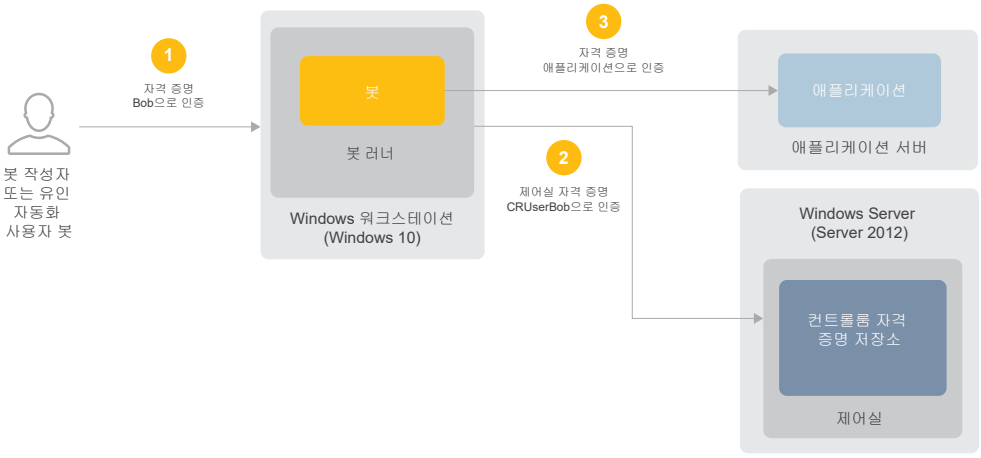

그림 3: 유인 자동화 시나리오의 인증 프로세스

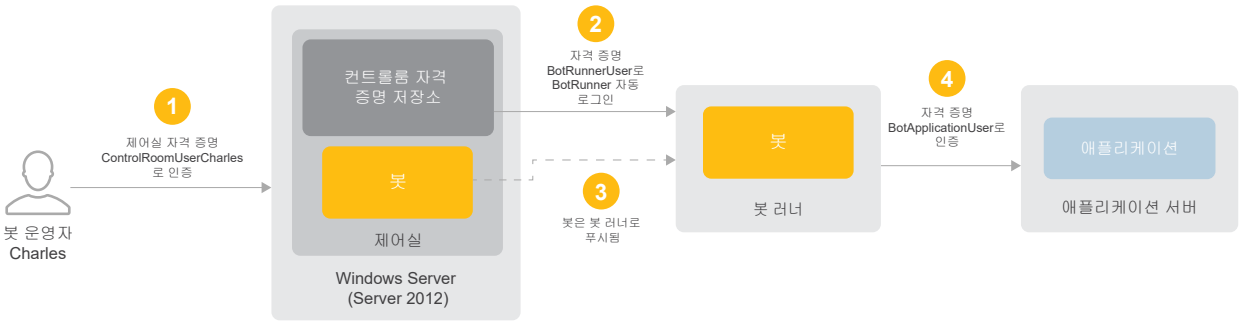

그림 4: 무인 자동화 시나리오의 인증 프로세스

인증 옵션 및 IAM 통합

Control Room 인증에 지원되는 옵션에는 LDAP을 사용하는 Active Directory, Kerberos를 사용하는 Active Directory, 내장된 자격증명 보관을 사용하는 로컬 인증이 있습니다(이후 섹션에서 설명).

엔터프라이즈 배포에 사용할 수 있는 기타 ID 및 액세스 관리 옵션은 다음과 같습니다.

+ SAML 2.0 기반 SSO(Single Sign-On)에 대한 지원
+ 타사의 권한 있는 액세스/자격 증명 관리 솔루션(예: CyberArk, One Identity, Thycotic)에 통합

포괄적인 역할 기반 액세스 제어

성공적인 인증은 Automation Anywhere Enterprise 보안 아키텍처에서 제공하는 필수 액세스 제어 적용의 첫 번째 수준에 불과합니다. 특히 최소 권한 및 업무 분리라는 핵심 원칙을 준수할 때는 세분화된 역할 기반 액세스 제어(RBAC)에 대한 지원도 마찬가지로 중요합니다.

RPA 플랫폼의 기본 아키텍처와 주요 기능 내에서 고려해야 할 5 가지의 역할(**표 1** 참조)이 있습니다. BotBuilder는 Bot Creator를 사용하여 비즈니스 로직을 캡처하고 해당 자동화를 생성합니다. BotBuilder는 테스트 애플리케이션 및 데이터 세트로 작업하므로 개발 단계 중에 프로덕션 시스템에 영향을 주지 않습니다. 개별 봇은 일반적으로 초기 개발 과정뿐만 아니라 관련 비즈니스 프로세스 및 대상 애플리케이션이 업데이트될 때마다 여러 반복과 버전을 거칩니다. 또한 BotTester는 Bot Creator와 협력하여 봇의 성능, 데이터 무결성 및 보안을 테스트함으로써 각 봇이 안전하게 작업을 수행할 수 있도록 합니다. BotTester는 프로덕션 데이터 및 애플리케이션을 실행하기 전에 봇의 두 번째 인증 단계 역할을 합니다.

일단 봇이 테스트를 거쳐 보안 검토를 받으면 BotPromoter는 BotBuilder/BotTester와 협력하여 프로덕션에서 사용해야 하는 봇의 버전을 지정합니다. 이는 사업부와 협력하여 봇을 예약하고 실행하는 BotOperator가 볼 수 있는 유일한 버전의 봇입니다. 또한 BotOperator는 발생한 런타임 문제를 해결하는 등 Control Room 내 봇 성능의 모니터링을 담당합니다. 마지막으로 RPA Admin은 구성 요소, 인터페이스 및 모든 역할/권한을 구성하는 등 플랫폼의 전반적인 관리를 담당합니다.

고급 업무 분리

이 일련의 핵심 역할은 RBAC에 대한 기본적인 출발점을 보여주지만 Automation Anywhere Enterprise 플랫폼 내에서는 훨씬 더 많은 업무 분리가 가능합니다. 관리자는 내장된 역할 생성 마법사를 사용하여 사용자 지정 역할을 손쉽게 정의할 수 있으므로 사용자 관리, 라이선싱, 자격증명 보관, Bot Runner 세트, 봇 일정, 봇 운영/대시보드, 감사 로그를 비롯하여 Control Room 객체 및 기능 전체를 설명하는 권한을 설정할 수 있습니다. 각 권한이 선택되면 마법사는 조건부/파생된 권한에 대한 단계를 동적으로 추가합니다.

예를 들어 봇 > 내 봇 보기 > 내 봇 실행 권한이 선택되면(**그림 5** 참조) 워크플로에서는 액세스 권한이 부여되는 특정 봇 폴더(즉, 봇 세트)를 나타내는 단계를 추가합니다. 최종적으로 가장 엄격하고 안전하며 규정 준수 규제가 까다로운 환경의 요구에 부응하기 충분한 세분화된 액세스 제어로 충실도 높은 역할을 수립할 수 있습니다.

역할	설명
RPA Admin	시스템 관리(구성요소, 역할, 인터페이스 구성)
BotBuilder	작업 편집기로 봇을 생성하고 기본 기능 테스트를 수행하는 비즈니스 프로세스 전문가
BotTester	기능 정확도, 성능 및 보안을 위해 봇을 검토하는 품질 보증 테스터
봇 프로모터	개발, 테스트 및 프로덕션 단계에서 봇을 승인하고 이동하는 관리자
RPAOperator	봇의 성능을 예약, 실행 및 모니터링하는 운영자

표 1: Automation Anywhere Enterprise의 기본 RPA 역할

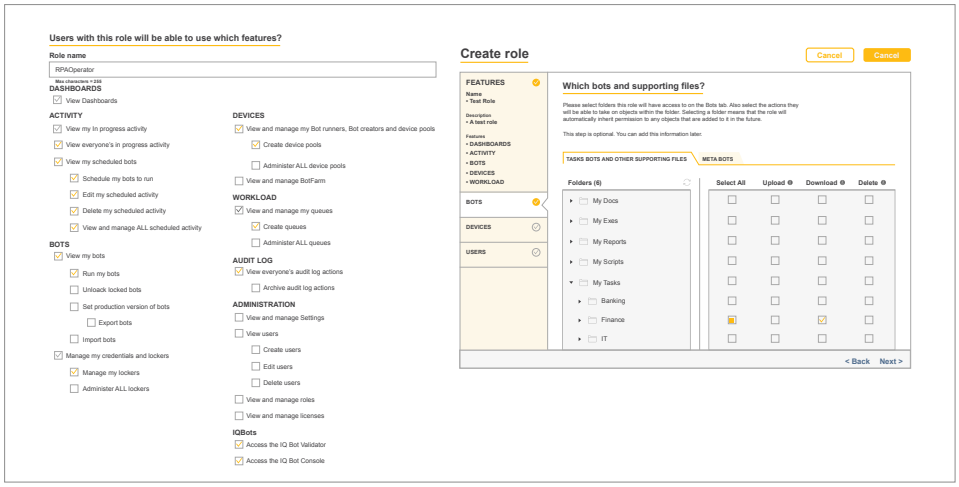

그림 5: 세분화된 인증을 통해 역할 생성

독립적 제어 평면

광범위한 RBAC 기능 외에도 Automation Anywhere Enterprise는 본질적으로 봇 개발 및 봇 실행 작업을 철저히 분리하는 아키텍처를 채택하여 논리적인 업무 분리를 제공합니다.

봇 생성자는 Control Room 내의 버전 제어 시스템을 통해 봇을 업로드와 다운로드만 할 수 있습니다. 동시에 봇 실행자는 봇 실행 작업으로 제한되며 봇 생성 및 테스트 기능에 액세스할 수 없습니다. 구조적으로 적용된 이 업무 분리는 최종적으로 비즈니스 프로세스 자동화를 실현하기 위해 개발자와 비즈니스 사용자 모두 (최소한) 필요하므로 미국 국립표준기술연구소(NIST) 모범 사례와 일치하는 이중 승인을 구성합니다.

독립적 처리 도메인

플랫폼의 RBAC 기능, 특히 대규모 엔터프라이즈를 위한 강력한 사용 사례는 독립적 처리 도메인을 구축하는 것입니다(**그림 6** 참조). 이는 Control Room 내의 해당 폴더에 원하는 각 도메인의 봇을 엄격하게 구성/저장하면 가능합니다.

해당 사례: 금융 애플리케이션과 관련된 봇은 재무 폴더에 배치되고 HR과 관련된 봇은 HR 폴더에 배치됩니다. 재무 부서의 봇 운영자는 재무 봇 및 재무 봇 실행자에 대한 권한만 할당받습니다. HR의 봇 운영자는 HR 봇 및 봇 실행자에 대한 권한만 얻으며 기타 처리/자동화 도메인의 경우에도 마찬가지입니다(**그림 6** 참조).

그 결과, 개별 운영자가 지정된 도메인 외부에서 봇을 보거나 운영할 수 없으므로 이번에는 OU/도메인 수준에서 업무 분리 및 관련 앱과 데이터의 분리가 더욱 심화되었습니다.

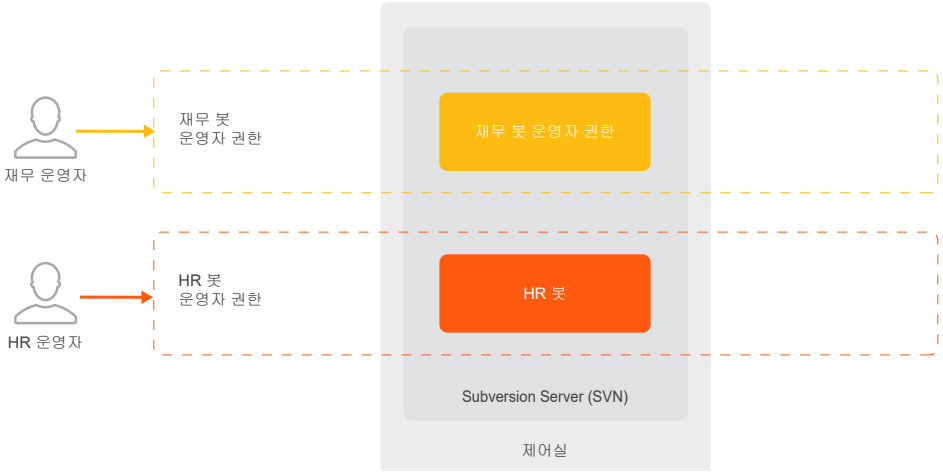

그림 6: 독립적 처리 도메인에 대한 지원

END-TO-END 데이터 보호

엄격하게 제어되는 환경에서는 다중 계층 인증 및 세분화된 액세스 제어가 필수적입니다. 비즈니스에 중요한 프로세스, 민감한 데이터 및 관련 암호(예: 자격 증명)의 기밀성과 무결성을 유지하는 데 필요한 end-to-end 데이터 보호도 마찬가지입니다.

Automation Anywhere Enterprise 플랫폼은 내장된 자격증명 보관을 사용하여 이 요구를 해결하고 정지 및 전송 도중은 물론 개별 시스템에서 사용하는 동안에도 데이터를 보호하는 광범위한 보호책을 제공합니다.

암호화 키 및 자격증명 보관

그림 7은 플랫폼에서 사용되는 기본 암호화 키와 자격증명 보관에 대한 관계를 보여줍니다. 모든 암호화는 FIPS 140-2, 레벨 1의 검증된 암호화 모듈을 사용하여 수행됩니다.

설치 도중에(**그림 7**의 왼쪽 부분) 시스템은 RSA 2048비트 퍼블릭/프라이빗 키 페어와 AES 256비트 키를 생성합니다. RSA 2048 페어의 프라이빗 키는 마스터 키라고 하며 AES 256 키는 데이터 키라고 합니다. 마스터 키는 시스템의 물리적으로 안전한 위치에 안전하게 보관하기 위해 설치 관리자에게 제공됩니다. 퍼블릭 키는 데이터 키를 암호화하는 데 사용됩니다. 그런 다음 퍼블릭 키와 암호화된 데이터 키는 모두 데이터베이스에 저장됩니다. 사용 중에 모든 키와 암호화된 데이터는 Microsoft Data Protection API(DPAPI)를 사용하여 암호화된 보안 메모리에 저장됩니다.

Control Room 시작 또는 재부팅 도중에(**그림 7**의 오른쪽 부분) 관리자는 마스터 키를 제공하라는 메시지를 확인합니다. 암호화된 데이터 키는 데이터베이스에서 검색되고 마스터 키를 사용하여 해독됩니다. 이제 데이터 키를 사용할 준비가 되었습니다. 시스템이 자격증명 보관에서 데이터를 저장하고 검색할 때 데이터 키는 해당 데이터를 암호화하고 해독하는 데 사용됩니다.

자격증명 보관은 모든 시스템 관리형 자격 증명과 중요한 시스템 구성 데이터를 저장하는 데 사용됩니다. 또한 조직의 자동화에 사용되는 기타 모든 민감한 데이터(예: 이름-값 쌍)를 저장하는 데 사용할 수 있습니다. 그 결과, BotBuilder는 자동화 내에서 직접 자격 증명 및 기타 민감한 데이터/인수를 하드 코딩하는 위험한 방법을 피할 수 있습니다.

정지 상태의 데이터 보호

자격증명 보관이라는 로컬 자격 증명을 암호화하고 봇이 사용하는 런타임 데이터를 선택할 뿐만 아니라 중요한 구성 변수와 통합 버전 제어 및 이메일 서비스와 관련된 세부 정보를 안전하게 저장합니다.

전송 중 데이터 보호

클라이언트 및 Control Room의 모든 네트워크 서비스는 TLS(Transport Layer Security) 1.2를 사용하여 구성 요소 간의 전송 중에 데이터 보안 및 무결성을 보장합니다.

Control Room에 대한 Bot Creator/실행자 인증에 사용되는 자격 증명은 TLS 보안 연결을 통해 제출되기 전에 암호화됩니다. 이 추가 암호화 계층은 네트워크 스택 문제(예: Heartbleed)를 방지할 뿐만 아니라 프런트 엔드 로드 밸런서에서 외부 계층 TLS 연결이 종료되는 구현에 대한 자격 증명 노출을 방지합니다.

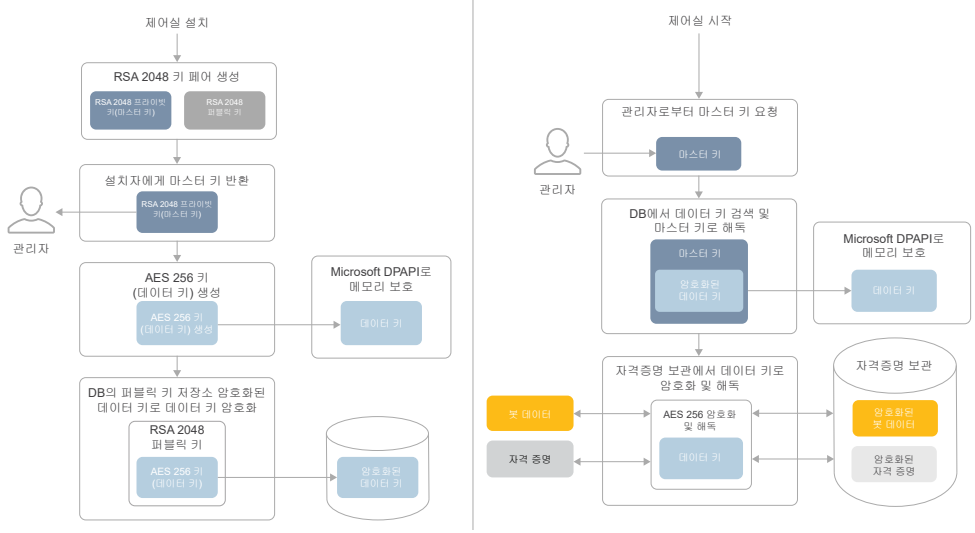

그림 7: Automation Anywhere Enterprise 암호화 아키텍처

사용 중인 데이터 보호

런타임 보안은 분산된 자격 증명 보호로 시작됩니다. 특히 봇 실행자에는 로컬 자격 증명 저장소가 없습니다. 자동화 내에서 사용하기 위해 자격증명 보관에서 동적으로 검색된 자격 증명 및 기타 데이터는 휘발성 메모리에서만 암호화된 형식으로 유지되며 관련 봇의 실행이 완료되면 삭제됩니다.

기밀 정보에 대한 무단 액세스(즉, 데이터 유출) 또는 런타임 중에 봇 변경을 방지하는 데 사용할 수 있는 기타 기능 및 구성 옵션은 다음과 같습니다.

+ 스텔스 모드 – 프로그램 창이 로컬 화면에 표시되지 않고 로그인한 사용자는 Bot Creator 및 봇 실행자에서 이미지 캡처를 비활성화할 수 있으므로 화면에 표시된 민감한 정보가 봇에 저장되는 것을 방지함
+ 입력 잠금 – 자동화가 실행 중인 시스템의 마우스 및 키보드를 비활성화하는 기능
+ 시간 제한 – 실행이 완료되지 않은 경우 자동화가 종료되는 시간 제한을 설정하는 기능
+ 중앙 제어 – Control Room 내에서 원격으로 실행되는 자동화 작업을 중앙에서 제어(즉, 일시 중지, 재개, 중지)하는 기능

보안 소프트웨어 개발 주기 (SDLC) 지원

자동화 환경에 대한 제어 및 보호를 극대화하기 위해 이전에 설명한 기본 배포 시나리오를 "확장"하여 FISMA, FedRamp, PCI DSS에서 요구하는 것과 같은 보안 소프트웨어 개발 주기(SDLC) 모범 사례를 제공할 수 있습니다. 결과적으로 고급 배포 모델은 개발, 사용자 승인 테스트(UAT) 및 프로덕션으로 각각 구성된 3개의 RPA 영역을 제공합니다(그림 8 참조). 각 영역은 서로 다른 역할과 권한이 부여된 여러 사용자 그룹으로 논리적으로 분리(격리)됩니다. 점선으로 표시된 수직선은 네트워크 세분화 및 방화벽을 나타냅니다.

기본 배포 모델과 마찬가지로 봇 주기는 개발에서 시작됩니다. BotBuilder가 봇에 만족하면 UAT BotPromoter는 봇을 개발 버전 저장소(SVN)에서 UAT 저장소로 전송합니다. UAT 영역의 유일한 목적은 봇의 정확도, 성능 및 보안을 테스트하는 것입니다. 봇이 승인 테스트를 통과하면 프로덕션 BotPromoter는 해당 봇을 프로덕션 영역으로 전송합니다. 이 시점에서는 프로덕션 상태를 실현하고 RPAOperator가 프로덕션 애플리케이션과 함께 사용할 수 있습니다. 이 프로세스의 각 단계에서는 서로 다른 역할과 권한이 부여된 관리자에 의해 확인 및 인증이 수행됩니다. 디지털 인력의 안정성, 확장성, 효율성, 안전성 및 호환성을 보장하기 위해 엄격한 업무 분리 및 다중 계층 제어가 계획에 따라 기본 제공됩니다.

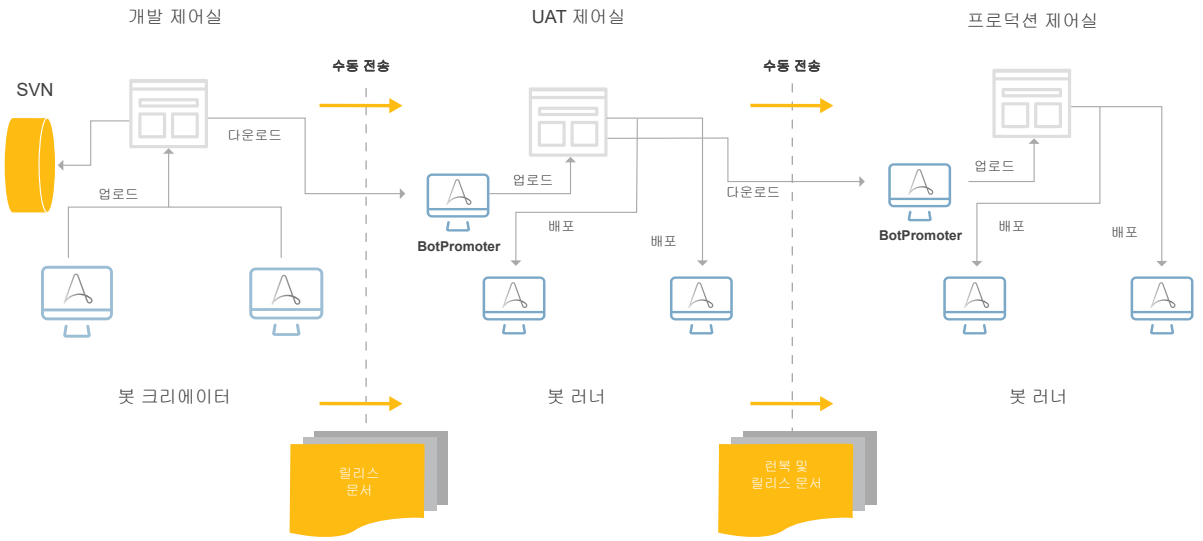

그림 8: 전체 SDLC 지원을 위한 고급 배포 모델

로깅 및 모니터링

포괄적인 감사 로깅, 모니터링 및 보고 기능은 뛰어난 IT 솔루션을 위한 보안 아키텍처의 필수적인 구성 요소입니다. Automation Anywhere Enterprise도 예외는 아닙니다.

플랫폼 전반에서 사용자, 봇, Bot Creator, 봇 실행자의 생성, 수정, 사용, 사용 중지 및 제거를 비롯하여 60개 이상의 사용자/엔터티 작업 유형에 대해 이벤트 세부 정보(대상, 내용, 시기, 위치, 성과)가 자동으로 캡처됩니다. 부인 방지는 자동 캡처, 특정 ID에 대한 각 활동의 결합 및 기본 읽기 전용 정책의 조합을 통해 구현됩니다. 또한 RBAC를 사용하여 처음부터 로그를 감사할 가시성이 있는 역할을 엄격하게 제어할 수 있습니다.

모니터링 관점에서 생각해볼 때 자동화된 대시보드 및 보고서는 Control Room 내에서 액세스할 수 있으며 비정상적인 활동(또는 자동화나 보안 팀이 관련이 있을 것으로 결정한 기타 모든 세부 사항)을 식별하고 경고하도록 사용자 지정할 수 있습니다. 또한 로그 내보내기 기능을 통해 조직에서 이미 사용 중인 다른 분석, 보고 및 사고 조사/응답 인프라(예: SIEM, UEBA, 고급 분석 도구)를 사용할 수 있습니다.

추가 엔터프라이즈 보안 및 복원력 기능

Automation Anywhere Enterprise는 다음을 통해 엔터프라이즈 보안 및 복원력 목표를 추가로 지원합니다.

+ 조직의 기존 고가용성/재해 복구(HA/DR) 인프라 및 프로세스에 원활하게 "적용"할 수 있는 분산된(유연한) 구성 요소 아키텍처
+ 플랫폼의 광범위한 RBAC 기능과 함께 매우 엄격한 변경 관리 정책 및 프로세스를 구현하고 적용할 수 있는 통합 버전 제어 시스템(Apache Subversion)
+ 플랫폼 코드 개발 중에 일반적인 공격(예: SQL 삽입 및 사이트 간 스크립팅)에 대한 취약성을 제거하는 데 도움이 되는 Hibernate 및 ReactJS 프레임워크와 같은 도구
+ 소프트웨어 취약성을 감지하고 제거하기 위해 지속적인 다중 도구, 다중 계층 검사가 필요한 코드 개발용 보안 계획/프로토콜

Automation Anywhere Enterprise에 속하는 이러한 기능과 기타 여러 제어, 보호 및 보안 기능에 대한 자세한 내용은 Automation Anywhere Enterprise: 보안 아키텍처에서 확인할 수 있습니다.

로봇 프로세스 자동화는 운영 비용을 줄이고 고객 만족도를 높이며 경쟁 우위를 확보하려는 현대적인 기업과의 약속을 지키기 위해 노력합니다. 시장을 선도하는 지능형 디지털 인력 플랫폼인 Automation Anywhere Enterprise는 성공을 이루는 데 필요한 안정성, 확장성 및 유용성 기능뿐만 아니라 전체 자동화 환경의 기밀성, 무결성, 사용 가능성을 유지하는 데 필요한 엔터프라이즈급 보안을 제공함으로써 이러한 이점과 기타 이점을 최대한 얻을 수 있도록 도와줍니다.

Automation Anywhere Enterprise 에 대한 자세한 내용은 다음 웹 사이트를 참조하십시오.
https://www.automationanywhere.co.kr/products/enterprise.